

ECONOMIC VALIDATION

# The Economic Benefits of Google Cloud Cross-Cloud Network

Providing Secure and Scalable Hybrid and Multi-cloud Network Connectivity While Reducing Complexity and Lowering Cost by up to 51%

By Aviv Kaufmann, Practice Director and Principal Validation Analyst  
Enterprise Strategy Group

May 2024

# Contents

Introduction .....	3
Challenges .....	3
The Solution: Google Cloud Cross-Cloud Network .....	5
Enterprise Strategy Group Economic Validation .....	6
Google Cloud Cross-Cloud Network Economic Overview .....	7
Use Case 1: Building Distributed Applications .....	7
Use Case 2: Delivering Internet-facing Applications .....	9
Use Case 3: Providing Secure Access for the Hybrid Workforce .....	12
Issues to Consider .....	15
Conclusion .....	16

## Economic Validation: Key Findings Summary

### Validated Benefits of Google Cloud Cross-Cloud Network



**Up to 40% lower cost to build and operate distributed applications**



**Up to 51% lower cost to deliver internet-facing applications**



**Up to 33% lower cost to provide secure access to the hybrid workforce with an integrated SSE stack**

- **Reduced Complexity:** By unifying operations with Google Cloud's cloud-native technologies; reducing the number of colocation sites, private connections, and cloud front ends and services to manage; and unifying security stacks.
- **Improved Security and Availability:** Improved security and availability for applications and users requiring access to multiple clouds and locations with a unified security stack that integrates into Google Cloud's own secure, scalable, and redundant cloud-native platform.
- **Cost Savings:** Our models predicted that customers could lower costs by 33% to 51% by using Cross-Cloud Network and cloud-native tools rather than traditional colocation or multiple clouds.

# Introduction

This Economic Validation from TechTarget's Enterprise Strategy Group focused on the quantitative and qualitative benefits organizations can expect from using Google Cloud's Cross-Cloud Network, built on the Cross-Cloud Interconnect (CCI) to deliver simple, secure, and cost-effective hybrid and multi-cloud network connectivity.

## Challenges

Network connectivity has become a critical consideration as more established organizations complete their successful initiatives toward becoming fully digitally transformed organizations and new businesses enjoy their success made possible through a scalable cloud-first approach. As businesses expand, integrate their technical capabilities, and merge technologies with established organizations, the network perimeter expands from the data center to the edge and across multiple clouds.

This places a burden on existing network teams and technologies to support a modern hybrid and multi-cloud approach that enables migrations of data and workloads between public and private clouds, as well as distributed applications and services across clouds and locations. Teams and technologies must also support data access from anywhere for modern throughput-intensive workloads like artificial intelligence and machine learning (ML). In addition, these teams must support an increasingly larger and more diverse hybrid workforce to provide secure access to resources and applications from any device and any location.

Enterprise Strategy Group found that the two most common drivers for organizations' current or expected use of multiple public cloud infrastructure service providers are to optimize performance and to increase their ability to scale applications,<sup>1</sup> and when deploying applications, networking is the most difficult challenge that they face as a result of using multiple cloud service providers (CSPs, see Figure 1).<sup>2</sup>

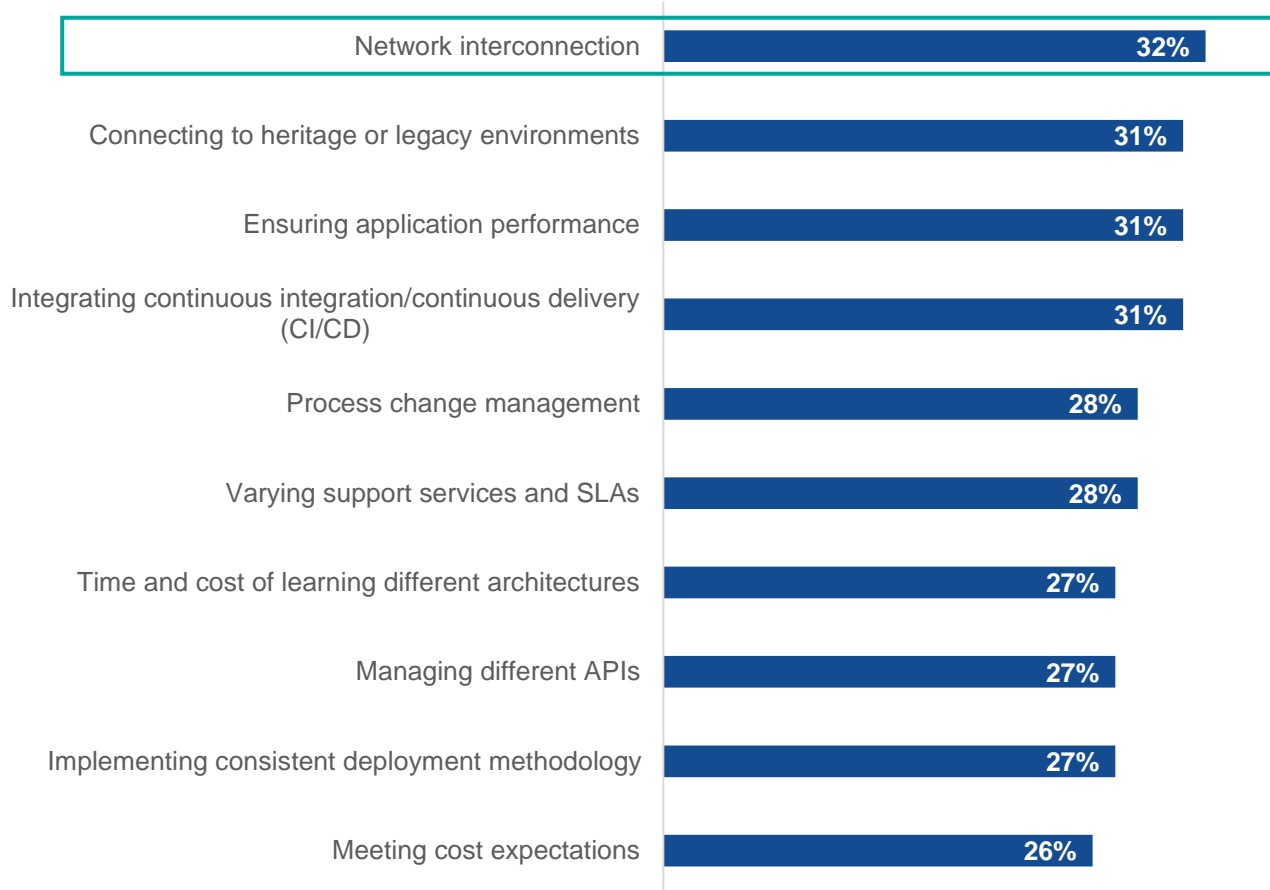
---

<sup>1</sup> Source: Enterprise Strategy Group Complete Survey Results, [Multi-cloud Networking Trends](#), February 2024.

<sup>2</sup> Source: Enterprise Strategy Group Complete Survey Results, [Distributed Cloud Series: The State of Infrastructure Modernization Across the Distributed Cloud](#), August 2023.

**Figure 1. Top 10 Challenges of Using Multiple CSPs**

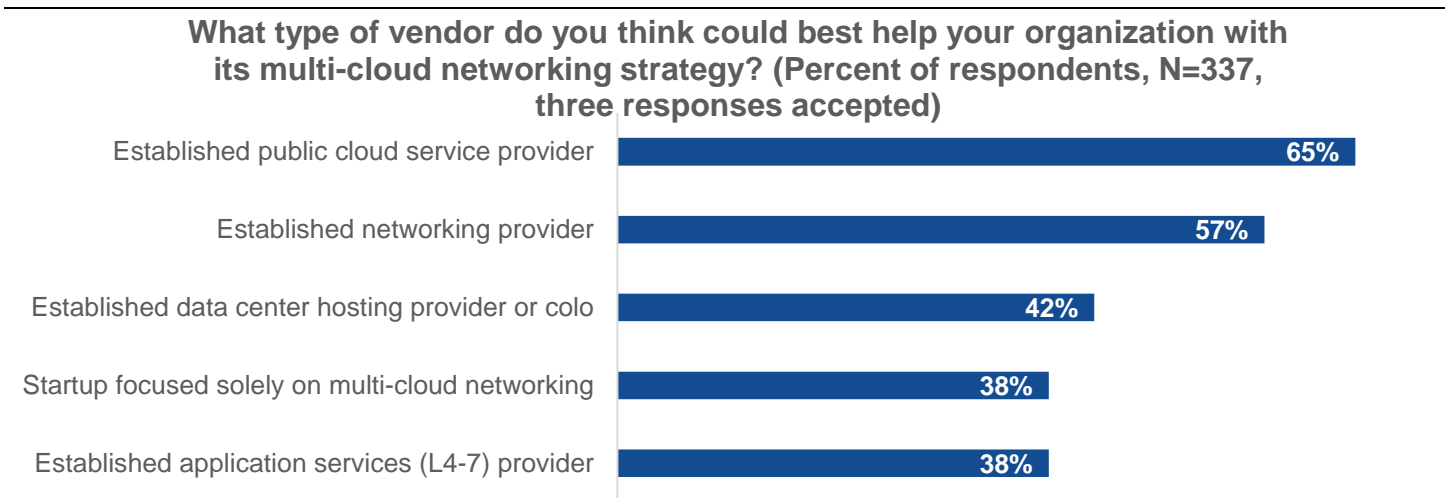
**In terms of new application deployment, what are the most difficult challenges your organization faces as a result of using multiple cloud service providers (CSPs)? (Percent of respondents, N=74, multiple responses accepted, top ten responses shown)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Operating multiple networks and security stacks across on-premises environments, colocation facilities, and multiple clouds independent of each other results in reduced security effectiveness, reduced performance, increased administrative complexity, and wasted spending. Organizations would be wise to consolidate onto a purpose-built network that is made to handle hybrid and multi-cloud operations. It must provide a consistent and scalable security stack, efficient routing, low-latency performance, operational simplicity, and minimized cost. When Enterprise Strategy Group asked organizations what type of vendor could best help with their multi-cloud network strategy, respondents overwhelmingly identified that an established CSP would be one of their top choices (see Figure 2).<sup>3</sup>

<sup>3</sup> Source: Enterprise Strategy Group Complete Survey Results, [Multi-cloud Networking Trends](#), February 2024.

**Figure 2.** Organizations Look to Established CSPs for Multi-cloud Networking Strategy Help

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

## The Solution: Google Cloud Cross-Cloud Network

Cross-Cloud Network is an open and programmable global cloud networking platform that enables simple connectivity between clouds and on-prem locations. It consists of existing and new products from Google Cloud and its partners, which all work together to simplify and accelerate the deployment of key use cases. Cross-Cloud Network is built on the three following tenets:

- **Open.** Cross-Cloud Network simplifies integration of partner products and services, providing organizations choice and fast time to market. It's also programmable, so users can customize the services that they need for their business.
- **Secure.** Google Cloud built ML-powered security products such as Cloud Armor and partnered with companies such as Palo Alto Networks to integrate advanced security technologies that can provide high threat efficacy with security posture controls.
- **Optimized.** Cross-Cloud Network optimizes workload performance with lower latency, higher throughput, and higher bandwidth. As organizations adopt generative AI, optimization is crucial for end-to-end performance.

Cross-Cloud Network provides any-to-any connectivity between more than 187 points of presence (POPs) and any private location through IPSec-based high-availability (HA) VPN tunnels, Partner Interconnect, Dedicated Interconnect, or software-defined WAN (SD-WAN) solutions enabled by Network Connectivity Center. Cross Cloud Interconnect (CCI) provides managed 10 Gbps or 100 Gbps links of high-bandwidth, dedicated physical connection between Google Cloud and another cloud service provider, with native encryption and a 99.99% service-level agreement (SLA). Supported service providers include Amazon Web Services, Microsoft Azure, Alibaba Cloud, and Oracle Cloud Infrastructure.

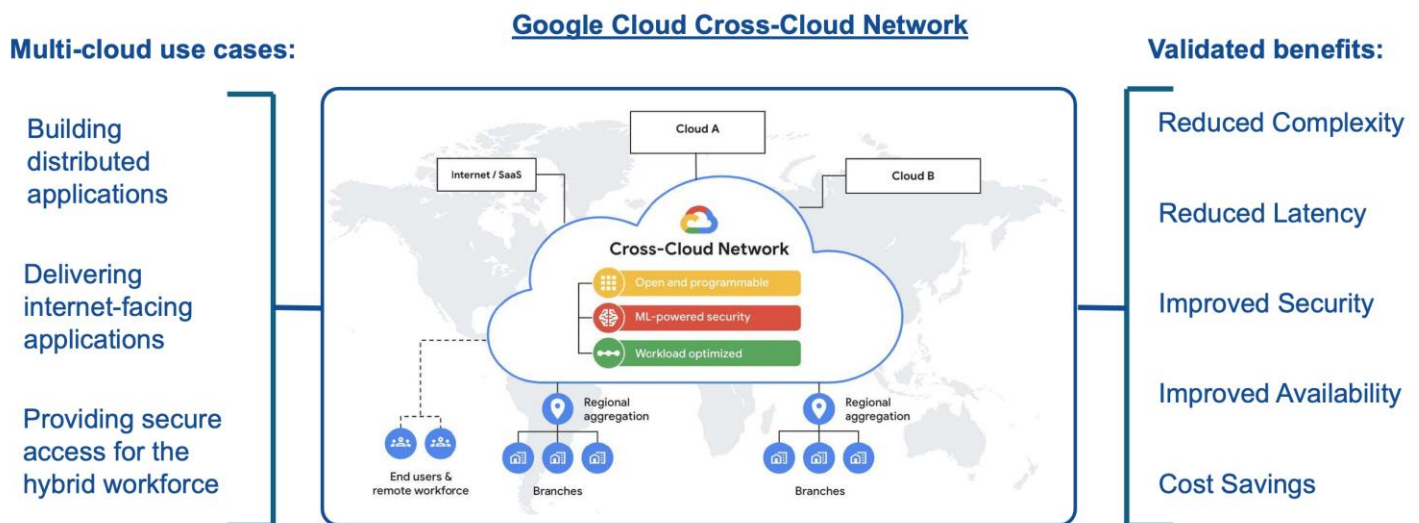
Security is provided through cloud-native, ML-powered security services in a consolidated connectivity and application security stack. Access to public applications is secured through a unified, global cloud front end that is protected by Google Cloud Armor's web application firewall (WAF). Employee access to applications to support hybrid work and application-to-application traffic is protected through a fully managed security stack delivered by Google Cloud's partners or through a cloud-native next-generation firewall (NGFW) service. Google Cloud NGFW Enterprise is a simple-to-deploy and simple-to-use, scalable, cloud-native, stateful inspection firewall engine that is enforced at each workload for the entire lifecycle. Identity and access management (IAM)-governed tags enable granular microsegmentation as well as hierarchical policy deployment and routing of traffic.



As shown in Figure 3, Cross-Cloud Network helps address the networking needs of the three most common use cases across clouds:

- **Building distributed applications.** Distributed applications break tasks up into smaller functions, external data services, or API calls that can be performed on the ideal platform before being recombined for a seemingly unified experience. Customers require network connectivity between clouds that is simple, secure, and cost-effective to provide seamless access to modern distributed applications that rely on data, resources, services, and APIs that are running in different clouds and locations.
- **Delivering internet-facing applications.** Customers that are running and hosting internet-facing applications in different public and private clouds require a unified, global front end that can ensure application end-user SLAs and security while reducing operational complexity, optimizing delivery and availability, and minimizing cost.
- **Providing secure access for the hybrid workforce.** In a hybrid workplace, employees have the flexibility to optimally combine remote work and on-site work according to their individual needs and that of the business. To support this, IT services must provide consistent access to all resources from any location. Hybrid workforces require top-of-the-line security services at the perimeter, delivered by a security service edge (SSE) provider and NGFW service that is best suited for the needs of the organization and applications.

Figure 3. Google Cloud Cross-Cloud Network



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

## Enterprise Strategy Group Economic Validation

Enterprise Strategy Group completed a quantitative economic analysis of Google Cloud's Cross-Cloud Network. Our Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages Enterprise Strategy Group's core competencies in market and industry analysis, forward-looking research, and technical/economic validation. We conducted in-depth interviews with end users and reviewed case studies to better understand and quantify how the Cross-Cloud Network and its underlying technologies have impacted their organizations. The qualitative and quantitative findings were used as the basis for an economic model that compares the cost and benefits of using the Cross-Cloud Network to optimize hybrid and multi-cloud networking across three common use cases.

## Google Cloud Cross-Cloud Network Economic Overview

Enterprise Strategy Group's economic analysis revealed that the Google Cloud Cross-Cloud Network generally provided its customers with some high-level significant savings and benefits in the following categories:

- **Reduced complexity.** Customers were able to reduce the complexity of their network operations by unifying those operations with Google Cloud's cloud-native technologies, reducing the number of colocation sites and private connections that they had to manage and secure, reducing the number of cloud front ends and services that they had to manage, and unifying their security stacks.
- **Improved security and availability.** Customers benefited from improved security and availability for applications and users requiring access to multiple clouds and locations by using a unified security stack that integrated into Google Cloud's own secure, scalable, and redundant cloud-native platform.
- **Cost savings.** Our models predicted that customers could lower costs by 33% to 51% using the Google Cloud Cross-Cloud Network and cloud-native tools rather than using colocation on-ramps with point security solutions and private connectivity to multiple clouds.

Enterprise Strategy Group validated how various customers have benefitted or plan to benefit by using the Google Cloud Cross-Cloud Network to optimize inter-cloud networking and security for the following three use cases: building distributed applications, delivering internet-facing applications, and providing secure access for the hybrid workforce.

### Use Case 1: Building Distributed Applications

Organizations are building powerful distributed applications that enable them to make the best use of services and resources that could reside in data centers, on multiple public clouds, at the edge, or in colocation environments and that could rely on integrations with SaaS providers. Information can be generated in one place, processed by tools in another, and delivered to end users and applications at a third. Managing network connectivity to all these separate resources can be complex and costly, especially when trying to ensure the levels of performance, security, and availability demanded by applications, employees, partners, and customers. Customers reported the following benefits when building distributed applications:

- **Dedicated private network connections between clouds.** Customers were able to leverage Cross-Cloud Interconnect (CCI) to handle dedicated private network connections between Google Cloud and other CSPs, eliminating the need for the customer to manage and pay for individual dedicated connections to each CSP through infrastructure in data centers or colocation environments. Customers could then access resources in all clouds by first connecting to Google Cloud through their choice of IPsec-based HA VPN tunnels, partner or dedicated Cloud Interconnect, or their choice of SD-WAN solution enabled by the Network Connectivity Center.
- **Improved network scale and performance.** Customers reported that, by using Google Cloud's high-performance, scalable networks; efficient routing; AI/ML-optimized networking; and cloud-native services like Google Cloud's Application Load Balancer with global access, they were able to scale their networks far beyond what they would be able to if managing multiple cloud networks and on-ramps. By reducing the number of "hops," they could easily scale applications and avoid many of the network latency issues that they had previously encountered. Customers did not run into issues with scalability, since every component of the Google Cloud Cross-Cloud Network is built for scale.
- **Improved network availability.** Once on the Google Cloud, customers' distributed applications and services continuously ran without encountering many of the issues and temporary disruptions to service that they had previously encountered. They reported fewer timeouts and said that they spent less time troubleshooting connectivity issues. Applications and data spent less time on the public internet and more on Google Cloud's own network, designed around network proximity and failover with periodic health checks, and thus avoided potential network connectivity issues with inter-VPC network address translation (NAT) for private IPs.

- **Improved network security.** The Google Cloud Cross-Cloud Network helped to ensure better security for distributed applications with more secure cross-cloud connectivity and more effective identification and protection against potential vulnerabilities. Customers were able to leverage Cloud Secure Web Proxy (SWP) for internet perimeter protection and to better secure internet egress traffic through Transport Layer Security (TLS) inspection and egress policy enforcement. All network traffic is encrypted and subject to policies enforced by Cloud NGFW and/or partner security offerings, with up to 95% threat protection efficacy.
- **Reduced complexity of network administration.** With Cross-Cloud Network, customers felt that they could spend less time managing, monitoring, and troubleshooting network issues for their distributed applications. They did not have to manage inter-cloud connectivity and could leverage cloud-native services that were built for scale and automation to reduce the complexity and amount of time that they spent performing individual tasks across a series of interfaces. One very large global customer shared that they might need to hire an additional 100 engineers if they were to try to build, secure, and manage similar network capabilities to what the Cross-Cloud Network provided them.
- **Improved quality of distributed applications.** For most organizations, the top benefit of building distributed applications on Cross-Cloud Network was validated by the improved quality they were able to achieve with their distributed applications. These applications were able to operate more securely with lower latency, greater reach, and improved uptime, providing richer customer experiences, improved productivity, and more effective business outcomes.

**“The Google Cloud Cross-Cloud Network allowed us to easily expand our distributed application to points of presence globally, helping to reduce latency for our users.”**

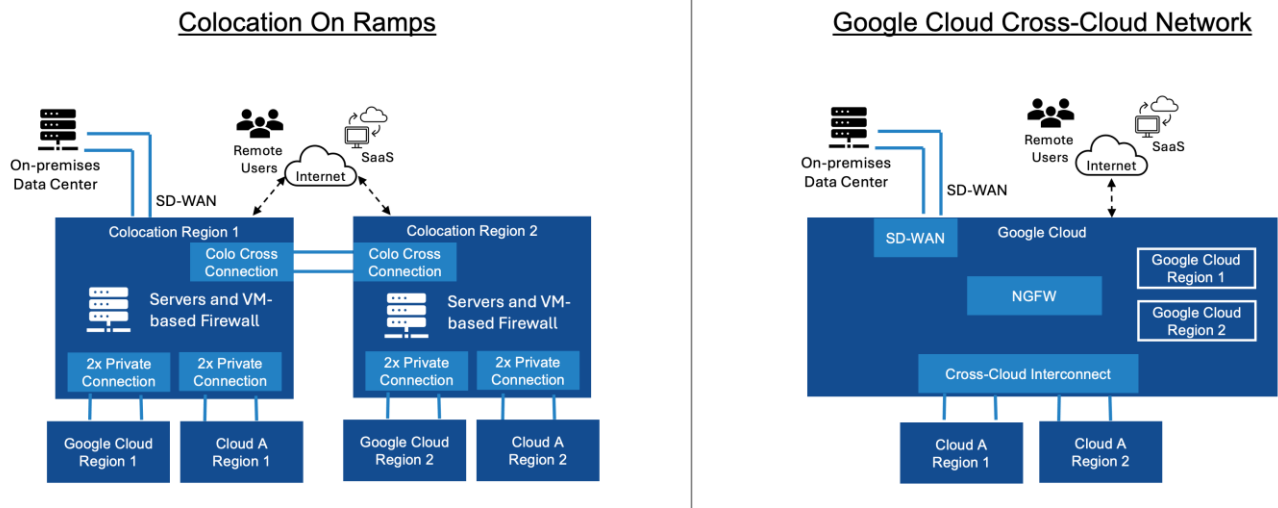
### *Cost Savings: Building Distributed Applications*

To demonstrate the cost savings that could be possible, Enterprise Strategy Group leveraged the information collected through vendor-provided material, public and industry knowledge of economics and technologies, and the results of customer interviews to create a three-year TCO/ROI model that compares the costs and benefits of building distributed applications before and after using Cross-Cloud Network.

The model assumed that a large organization was building distributed applications that leveraged data, services, and resources located in their on-premises private clouds, Google Cloud, another public cloud provider (Cloud A), and some SaaS service providers. We assumed that the global organization required cloud access across two regions for global availability and that the data centers were connected to colocation facilities using carrier connections and their current SD-WAN solution, with server-based, virtual firewall solutions and dual private connections to each cloud vendor in each region. Internet users and SaaS providers were accessed through the public internet.

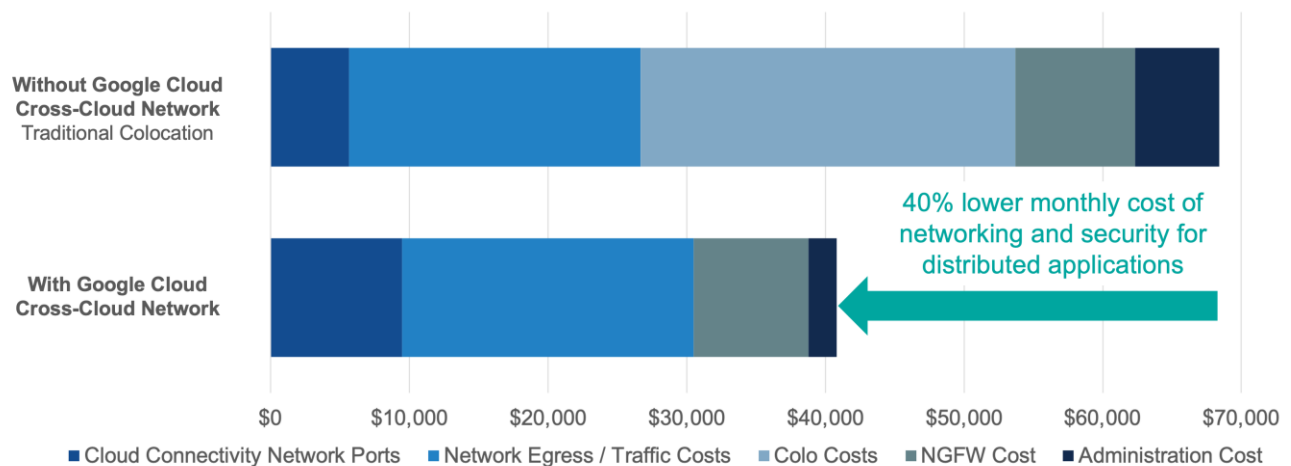
After moving to Google Cloud's Cross-Cloud Network, the organization was able to eliminate the need for colocation, instead connecting directly to Google Cloud through carrier connections and their SD-WAN via the Google Cloud Network Connectivity Center. Once on the Google Cloud, they leveraged the CCI to connect to each of the other public cloud regions. This scenario is shown in Figure 4.



**Figure 4.** Use Case Diagram: Building Distributed Applications

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As shown in figure 5, our models predicted a 40% lower expected monthly cost after using the Google Cloud Cross-Cloud Network. The cost of using the CCI resulted in higher port costs, but cost savings was provided by eliminating the need for colocation and by requiring 66% less management effort to ensure scalable and secure network connectivity.

**Figure 5.** Savings When Building Distributed Applications

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

## Use Case 2: Delivering Internet-facing Applications

Some organizations have the need to deliver internet-facing applications that are hosted on multiple cloud providers. This may be to take advantage of best-of-breed tools and services on each cloud, because their data resides in multiple clouds, because the organization inherited applications after mergers, because they wish to support applications running on each cloud's marketplace, or for another reason. But managing application front

ends, load balancers, security and governance, and data egress for each cloud provider can become complex. The Google Cloud Cross-Cloud Network can provide a unified global front end and scalable technology stack that helps reduce complexity, accelerate performance, and reduce cost. Customers reported the following benefits when delivering internet-facing applications:

- Improved end-user experience.** Customers were able to provide a single, global front end to direct and optimize the flow of data and traffic to and from any application, anywhere. The CCI provided high-speed connectivity to and from other public clouds when needed. The end users of their applications enjoyed improved performance, reliability, and security, as well as a better overall experience with the application. For internal-facing applications, this could mean improved productivity, while, for revenue-generating applications, this could mean improved customer satisfaction and retention, fewer support issues, and increased market share.
- Improved application front-end performance.** Cross-Cloud Network provides a customizable, global load balancer and traffic path optimization that ensures consistent, low-latency application front-end performance, regardless of where the application resides. For applications requiring even better regionalized performance, Google Cloud CDN and Media CDN could accelerate application performance even more by bringing web and video content closer to application users.
- Improved application front-end security and reliability.** Cross-Cloud Network helped to ensure more secure internet-facing application delivery, since all traffic to all clouds passed through Cloud Armor's ML-powered adaptive protection, which provided faster response to distributed denial-of-service (DDoS) attacks. Security was enforced for all traffic through automated deployment of ML-powered rules and mutual TLS client-side authentication for internet users that automatically verifies the client identity in a similar way to how server authentication works. Administrators were able to manage front-end security consistently and simply on one cloud instead of many, and they leveraged service extensions that provided custom monitoring and logging of network health to ensure end-to-end network health and application uptime.
- Improved application scale and reach.** Cross-Cloud Network made it easier for organizations to deliver scalable internet-facing applications by reducing the number of front ends, load balancers, WAFs, DDoS protection tools, and CDNs that developers and operators had to manage and plan for because Cross-Cloud Network could handle some of this in one cloud rather than in multiple clouds. Developers and operators benefitted from the automation solution toolkit and built-in automation for Cloud Armor, Cloud Load Balancing, Cloud CDN and Media CDN, and other functions into CI/CD platforms. Customers were able to better develop and ensure application scale and reach, regardless of where their application resided.
- Cost savings.** By unifying internet-facing applications with a global front end built for scale and programmability, customers were able to lower costs of separate and redundant cloud services for front-end load balancing, DDoS, and WAF protection, as well as simplify operations for cloud network and security administrators through built-in automation for scale and elimination of redundant activities across clouds.

**“After moving to the Google Cloud Cross-Cloud Network, we were able to reduce end-user network latency for our application by 20%.”**

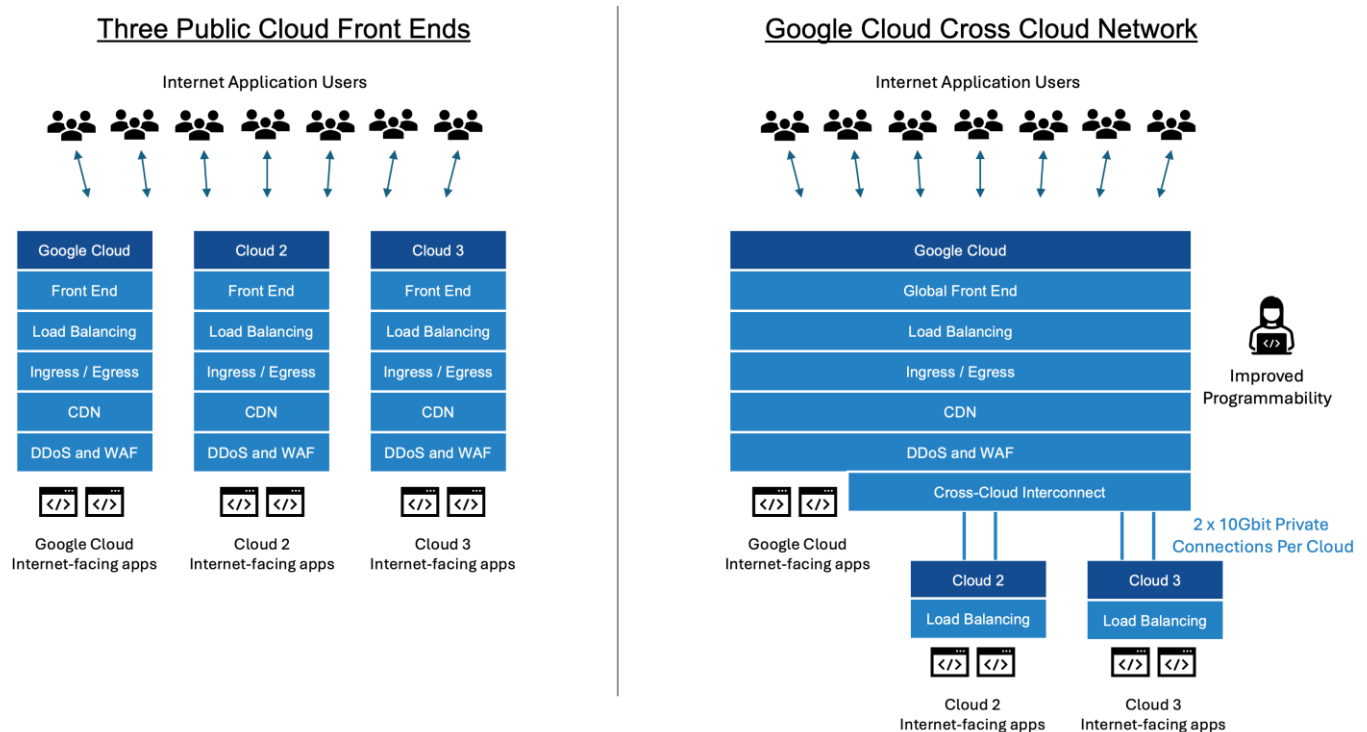
**“We have been able to reduce our time to mitigate security issues from tens of minutes to under five minutes with Google Cloud’s security automation.”**

**“Once the traffic enters the Google Cloud Cross-Cloud Network front end, it can then go to multiple cloud providers or the data center without going back out to the internet.”**

### Cost Savings: Delivering Internet-facing Applications

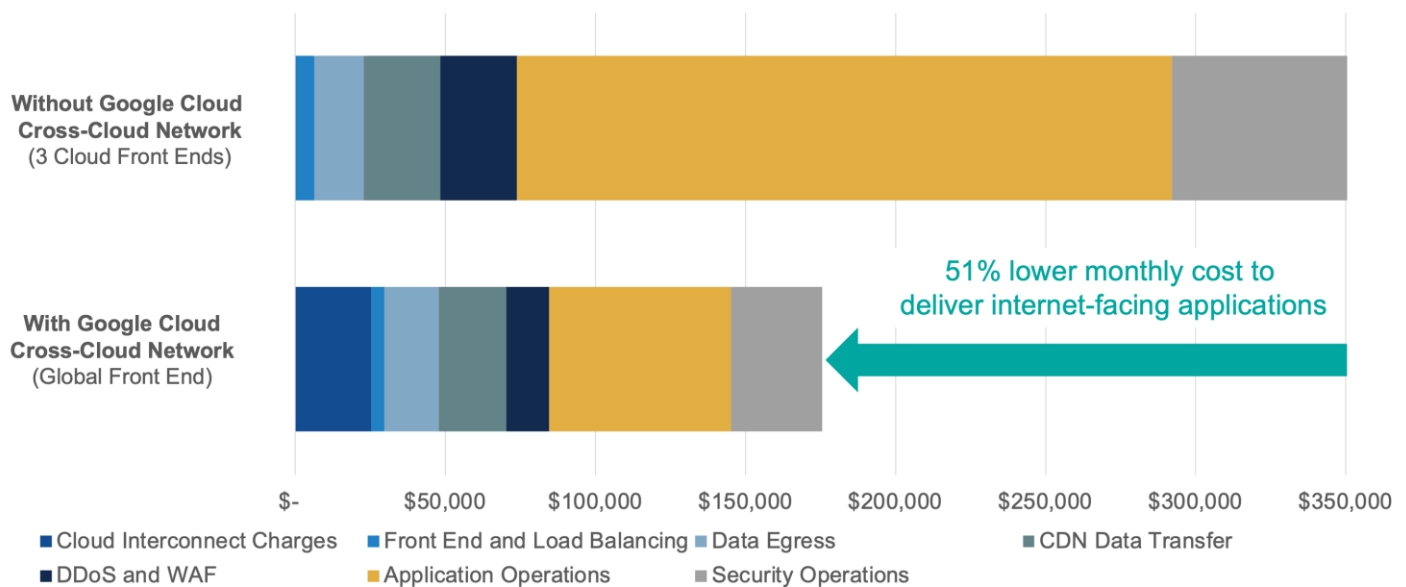
Our modeled scenario assumed that an organization currently had two internet-facing applications running in each of three public clouds (a total of six applications). To date, the organization managed each cloud independently, managing front-end and application load balancing across two regions, inbound and outbound traffic through load balancers and WAFs, and CDN traffic for 60% of their data. The organization then consolidated to a single global front end on Google Cloud's Cross-Cloud Network, handling global traffic, load balancing, CDN, DDoS, and WAF rules for all six applications using dedicated CCI connections to other cloud providers. This scenario is shown in Figure 6.

**Figure 6.** Use Case Diagram: Delivering Internet-facing Applications



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Our cost analysis predicted that, by providing a global application front end via Cross-Cloud Network instead of continuing to operate three separate cloud front ends, costs could be cut in half. Like the first scenario, there would be additional charges for operating dedicated connections using the CCI to the other two clouds, but the Google Cloud Cross-Cloud Network could help lower egress charges by 3%, front-end load balancing costs by 29%, CDN data transfer costs by 12%, DDoS and WAF costs by 44%, and application network and security administration costs by a total of 67%. The results of our cost analysis are shown in Figure 7.

**Figure 7.** Savings When Delivering Internet-facing Applications

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

### Use Case 3: Providing Secure Access for the Hybrid Workforce

With more workers than ever choosing to work in a remote or hybrid manner, organizations must find ways to securely provide access to applications, data, and resources that can reside on premises, across multiple public clouds, and on the internet. Providing secure access for employees relies upon multifaceted policies and processes that include educating employees, securing endpoint devices, encrypting network traffic, and verifying user and device identity. Securing user traffic that can originate and access resources anywhere can be very difficult for security teams to manage with consistency, which increases risk of vulnerabilities. Cloud-based SSE frameworks combine network and security functions into an easy-to-manage stack that secures access to the web, cloud services, and private applications. However, if SSE stacks are redundant or are not designed for optimal network placement, this can result in reduced latency that is noticeable to end users. Customers securing access for the hybrid workforce reported the following benefits:

- **Improved hybrid workforce security.** Cross-Cloud Network provided a common network and security solution to better secure users and traffic as well as deliver low latency across on-premises environments and multiple cloud networks. Google Cloud Armor provided a centralized and secure WAF and DDoS protection for all network traffic, and Google Cloud has partnered with some of the top security vendors to natively deliver integrated identity-aware proxy and SSE stacks that do not affect application performance. This results in fewer exploitable vulnerabilities stemming from hybrid workforce access and less impact to worker connectivity and productivity.

**“Google Cloud allows us to scale to meet the need of large spikes in traffic that we have seen during a security event. We could not scale resources to keep up with this volume of traffic with our homegrown security stack.”**

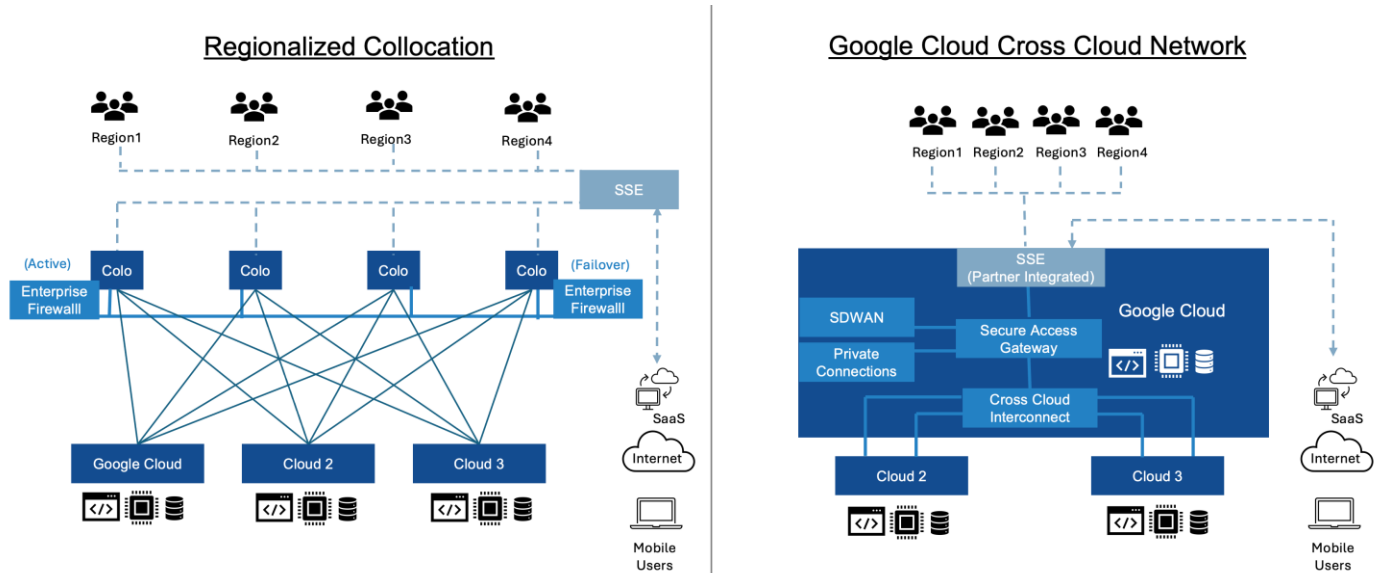
- **Reduced complexity.** Because Cross-Cloud Network and Google Cloud's partners provided a standardized cloud-native and integrated SSE stack for all users across all clouds and locations, it was easier for network teams to manage and operate security for their hybrid workers than it would be if they relied on multiple point solutions to secure each location and each cloud. Security vendors' leading SSE stacks were integrated into Google Cloud's own cloud-native stack, which made it very easy to deploy and scale. The SSE stack could also be fully managed by security partners on the Cross-Cloud Network, further reducing administrative burden and enabling existing resources to focus on other activities. This also reduced the need to scale security team resources and knowledge as the operations grew.
- **SSE stack standardization.** Organizations were given the flexibility to choose which SSE stack made the most sense for them from some of the top security partners, including Palo Alto Networks, Fortinet, and others. This enabled them to continue to leverage the in-house SSE expertise, integrations, and automations that they were used to across all clouds and on-premises locations, without having to make new investments in training or spend effort customizing or modifying existing tools and processes.
- **Reduced latency of SSE stack.** The unified and cloud-native SSE stack reduced the need to create and manage tunnels and overlay networks to redirect traffic to and from other networks to secure and authenticate users and traffic. With all traffic directed to Cross-Cloud Network first, traffic was secured and could securely pass to on-premises locations and other cloud networks through private and secure connections, without having to be redirected or pass through individual SSE stacks at each location. This minimized the small but noticeable delays when hybrid users were accessing applications and resources. Customers reported up to a 35% reduction in latency, which meant an overall better customer experience and less impact to hybrid operations.

**"We are able to leverage Google Cloud and their security partners' existing knowledge of bad actors and attack patterns to be able to better protect ourselves."**

#### *Cost Savings: Providing Secure Access to the Hybrid Workforce*

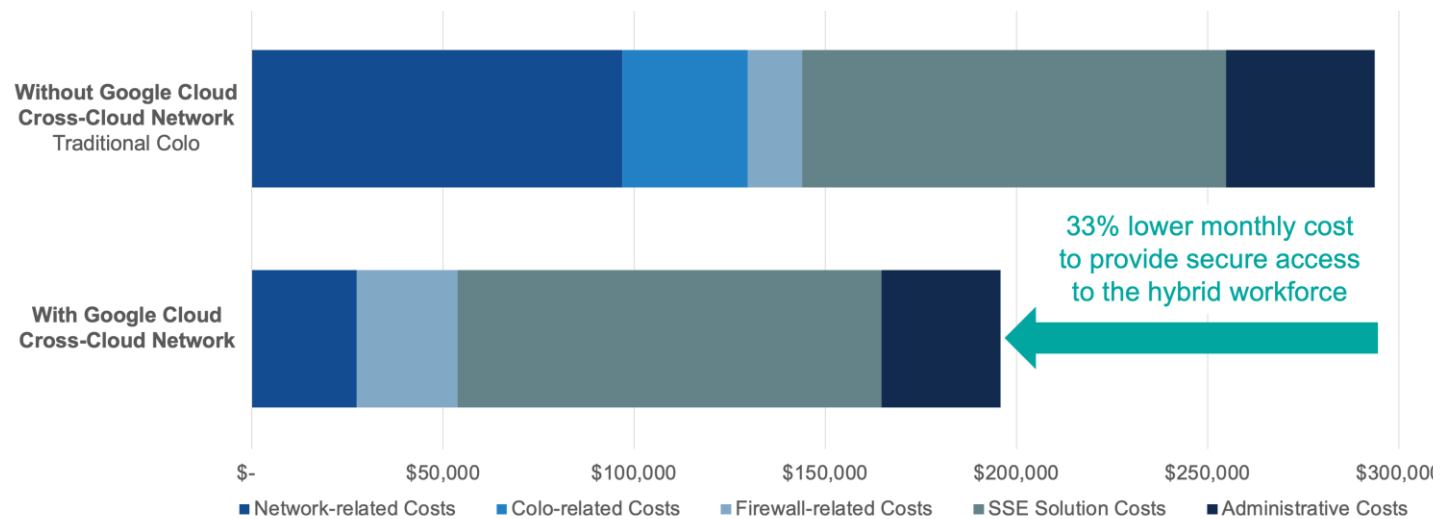
This modeled scenario assumed that an organization wanted to provide secure access to 6,000 hybrid users across four regions. A leading SSE provider was used to secure the perimeter, providing secure traffic and access among users, devices, SaaS applications, and private networks. Figure 8 shows this scenario.



**Figure 8.** Use Case Diagram: Providing Secure Access to the Hybrid Workforce

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Our model considered the cost to operate four colocation facilities in each region to provide appliance-based firewall security and cloud on-ramps to access resources on each of three cloud providers. By using the Google Cloud Cross-Cloud Network in conjunction with an SSE provider offering that integrates with the cloud-native services like the secure access gateway, the organization can minimize the traffic sent over the internet and reduce the number of hops required, resulting in reduced security latency. In addition, the CCI reduced the number of private cloud connections required from 12 to only four, helping to significantly lower monthly networking spending by 72%. We predicted a conservative 20% reduction in administrative costs after modeling the periodic work required to operate the four separate colocation networks, private connections, SSE connections, and physical firewalls versus using the cloud-native tools on Google Cloud. SSE costs were the same for each scenario. They were modeled based on the assumption of 6,000 users and 3 Gbps of total expected traffic and made up a significant portion of the total spending. As is shown in Figure 9, our models predicted a 33% lower monthly cost to provide secure access to the hybrid workforce.

**Figure 9.** Savings When Providing Secure Access to the Hybrid Workforce

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

## Issues to Consider

While our models are built in good faith upon conservative, credible, and validated assumptions, no single modeled scenario will ever represent every potential environment. The Google Cloud Cross-Cloud Network provides significant benefits and value to organizations looking to deliver secure, scalable, and cost-effective connectivity between multiple clouds and locations. Enterprise Strategy Group recommends that you perform your own analysis of available products and consult with your Google Cloud representative to understand and discuss potential implementations as well as the differences between alternatives proven through your own proof-of-concept testing.

## Conclusion

Secure network connectivity is perhaps the most important yet least understood factor in delivering modern applications and supporting a hybrid workforce. Making sure that people, devices, and resources can communicate across clouds and locations is not enough. There is much to consider around network latency, resource efficiency, management complexity, scalability, and security. The Google Cloud Cross-Cloud Network provides an opportunity for organizations looking to solve many of the potential problems around deploying, scaling, and securing network services for applications and users across multiple locations, clouds, and technologies.

Enterprise Strategy Group validated the savings and benefits that customers have seen when using the Google Cloud Cross-Cloud Network to help in three use cases, including building distributed applications, delivering internet-facing applications, and providing secure access to the hybrid workforce. These organizations were able to reduce cost and complexity, while also lowering network latency and reducing risk to the organization. Our models predicted that organizations could potentially reduce the total cost of multi-cloud and distributed networking for these use cases by 33% to 51%. Most of these savings are the result of reducing management complexity, consolidating traffic, minimizing time spent on the public internet, reducing the number of private connections and on-ramp locations that must be managed, and unifying the security stack. If your organization is looking for a secure, scalable, and cost-effective multi-cloud network solution, Enterprise Strategy Group recommends that you consider the Google Cloud Cross-Cloud Network.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).

---

#### About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 [contact@esg-global.com](mailto:contact@esg-global.com)

 [www.esg-global.com](http://www.esg-global.com)